Forticonverter V4.2.0 Release Notes

FortiConverter V4.2.0 Release Notes

September 3rd 2013

33-420-0217152-20130903

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log **4**
Introduction **5**
System Requirements **5**
Supported Vendors 5
Check Point 5
Juniper 5
Cisco PIX/ASA/FWSM 5
Cisco IOS 6
Sonicwall 6
Supported Conversions **6**
Check Point 6
Cisco 6
Juniper 6
Sonicwall 7
New Features **7**
Installing FortiConverter on a Windows computer 8
System Preconditions 11
Resolved Issues **14**
Pre-Conversion Technical notes **15**
Check Point Configuration File 15
Cisco Configuration File 15
Juniper Configuration File 15
Sonicwall Configuration File 15
Conversion Caveats **16**
Check Point 16
Juniper 17
Cisco 17
Sonicwall 18
Known Issues **20**
Known Bug References **20**

Change Log

Date	Change Description
2013-09-03	Initial Document Creation
2013-09-05	Revised Document
2013-09-17	Revised Document

Introduction

The FortiConverter product is a software only solution running on Windows platforms, allowing for the conversion of numerous vendors firewall configurations into Fortigate compatible configuration. This is the second generation of FortiConverter as the first version was available as a Web application and allowed for the uploading of configurations. This version is only available as stand alone. The software currently supports conversion from Cisco, Check Point, Juniper and Sonicwall. The software will run on a trial basis however it will not support Sonicwall configurations and will only support conversion of 100 policies additionally the tuning functionality will not be available. A license must be purchased and installed for full functionality.

SKU	Description
FC-10-CON01-401-01-12	1 Year Multi-vendor Configuration Conversion Tool (requires MS Windows) to create FortiOS configuration files
FC-10-CON01-401-02-12	1 Year Renewal Multi-vendor Configuration Conversion Tool (requires MS Windows) to create FortiOS configuration files

System Requirements

The FortiConverter software is designed to run on the following Windows platforms

- Microsoft Windows 8 (32-bit and 64-bit)
- Microsoft Windows 7 (32-bit and 64-bit)
- Microsoft Windows Vista (32-bit and 64-bit)
- Microsoft Windows XP (32-bit)

Supported Vendors

Firewall configurations are supported from the following vendors

Check Point

Models: Smart Center
OS: NG FP1 (4.0) to NGX R65/R70/R71/R75/R76

Juniper

SSG ScreenOS 5.x 6.x

SRX JunOS 10.x 11.x 12.x

Cisco PIX/ASA/FWSM

PIX: 5.x 6.x 7.x 8.x

ASA: 7.x 8.x

FWSM: 2.x 3.x 4.x

Cisco IOS

OS: 10.x 11.x 12.x 15.x

Sonicwall

Model: NSA
OS: SonicOS Enhanced 5.x

Supported Conversions

Check Point

Interface (physical, logical, loopback, pppoe)
Addresses /Address Group
Service/Service Group
Schedules
Rule
NAT (Automatic NAT/ Rule NAT)
VPN (IPSEC)
local user/User group
AAA server (Radius/Tacacs+/LDAP)
Static Route

Cisco

Interface(physical, logical, loopback, pppoe , tunnel)
Address/Address Group
IP pool
Time-range
DHCP server
Service/Service Group
Static Routes
ACL
NAT
VPN (IPSEC, PPTP/L2TP)
Local user/User group
AAA server (Radius/Tacacs+/LDAP)

Juniper

Interface (physical, logical, loopback, pppoe , tunnel)
Zone
DHCP server/client/relay
Policy
NAT
Address/Address group/fqdn
IP pool
VIP/MIP

Service/Service Group
Static Routes
VPN (IPSEC, PPTP/L2TP)
Local user/User group
AAA server (Radius/LDAP)

Sonicwall

Interface(physical, logical, loopback, pppoe)
Zone
DHCP server/client/relay
Policy
NAT
Address/Address Group
Services/Service Group
Static Routes
Schedule
Local user/User group

New Features

New Features are listed below. For a full list of features please refer to FortiConverter Documentation.

- Support for Juniper JunOS
- Support Fortimanager 5.x Output
- Support Checkpoint Smartcenter “policy package” of rulebases.fw
- Support for Checkpoint Smartcenter support to R76
- Add option of discarding all unreferenced firewall objects
- Support Checkpoint Negate Cell
- Support New Object/Object Group service Definition for Cisco ASA 8.3 and higher
- Support Keywords “ip domain”, “ip domain-list”, “ip host” and “ip name-server” for Cisco IOS
- Add support for IOS EZVPN conversion
- Support VPN “group-policy” and “tunnel-group” commands for Cisco PIX/ASA
- Add Option for policy generated with real comments and auto generated comments

Installation

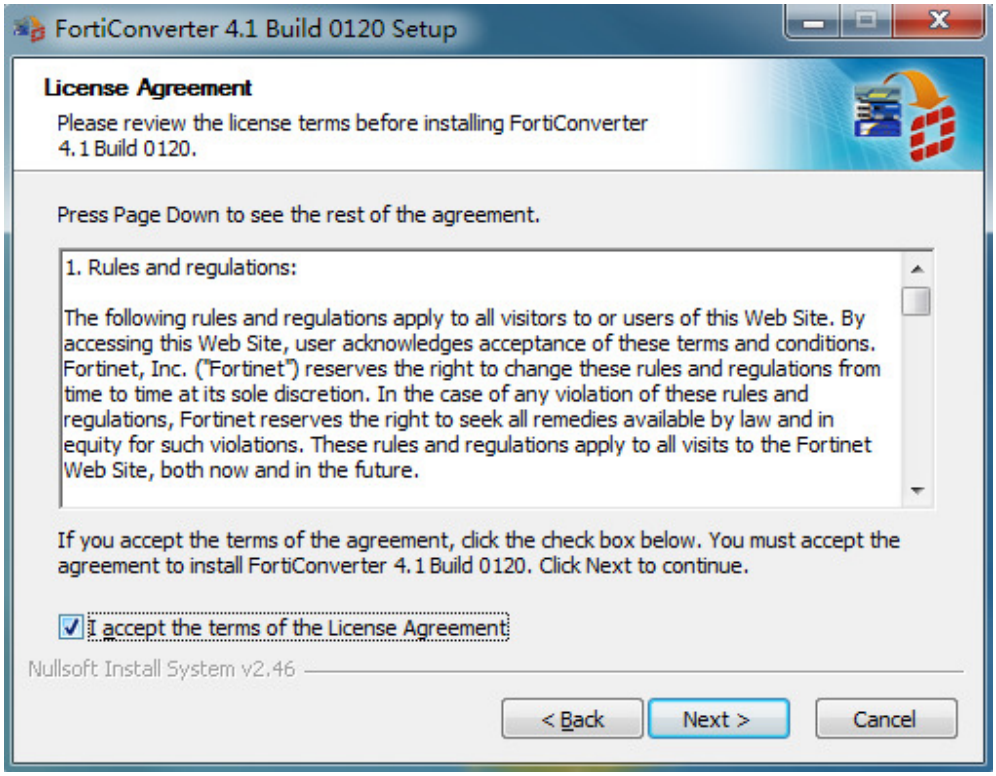
Installing FortiConverter on a Windows computer

The following instructions will guide you through the installation of FortiConverter on a Windows computer.

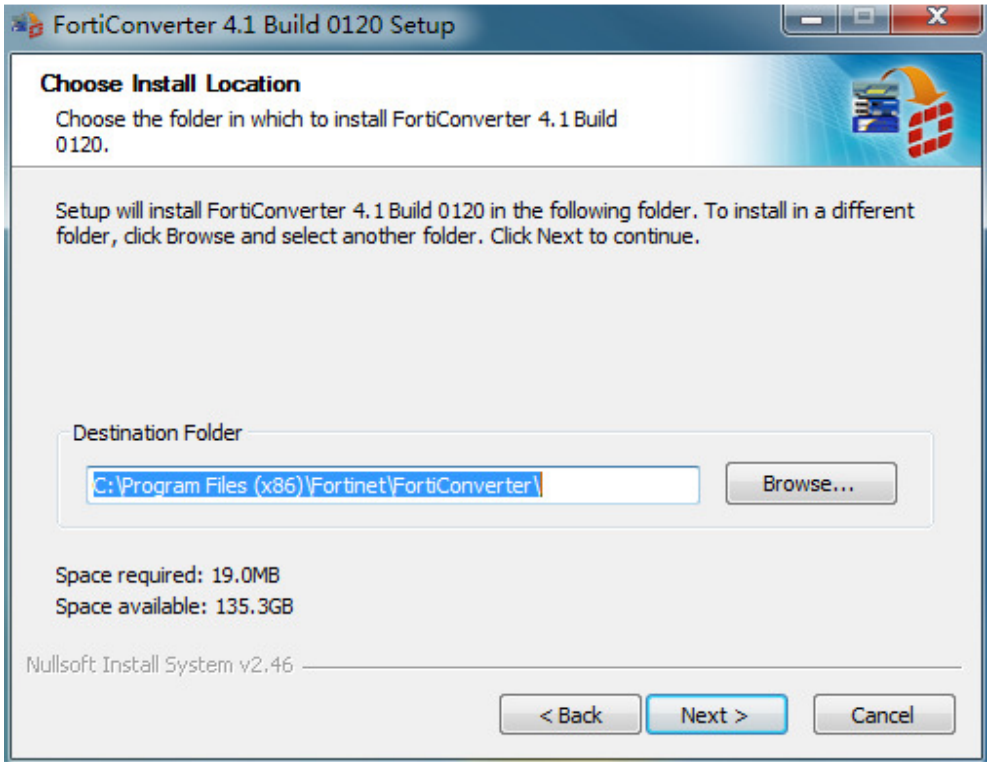
To install FortiConverter

1. Double-click the FortiConvertertSetup executable file to launch the setup wizard. The *Setup Wizard* will install FortiConverter on your computer.

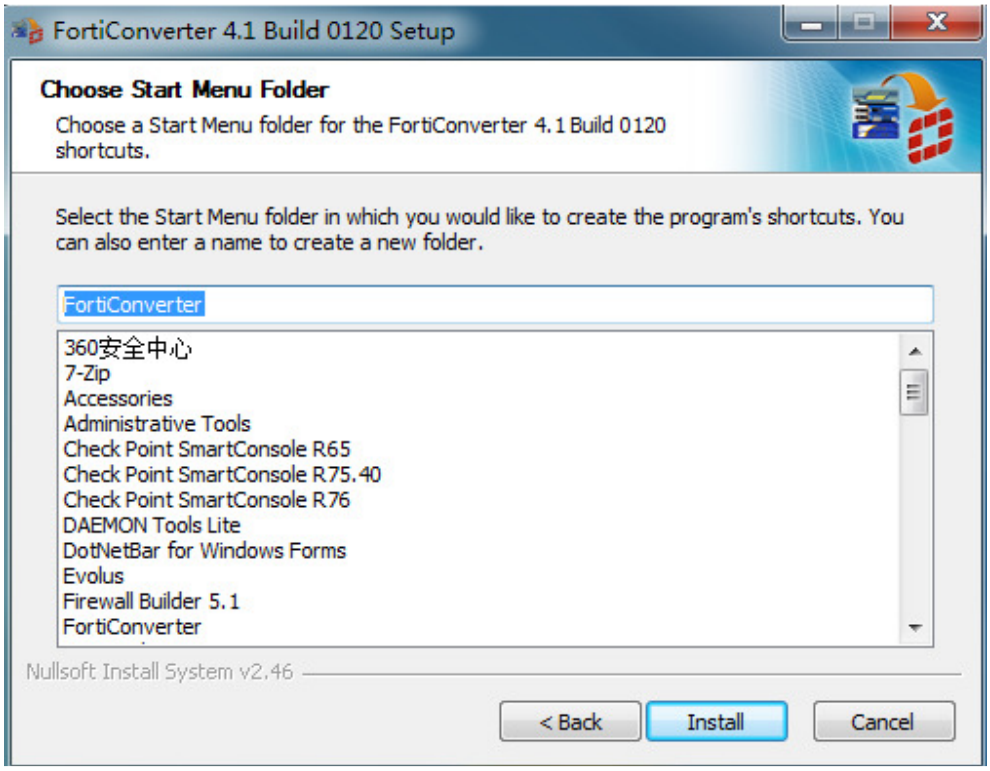
2. Read the license agreement and select *Next* to continue.



3. Select *Browse* to choose an alternate folder destination for installation. Select *Next* to continue.



4. Select to choose start menu folder and select *Install* to continue.

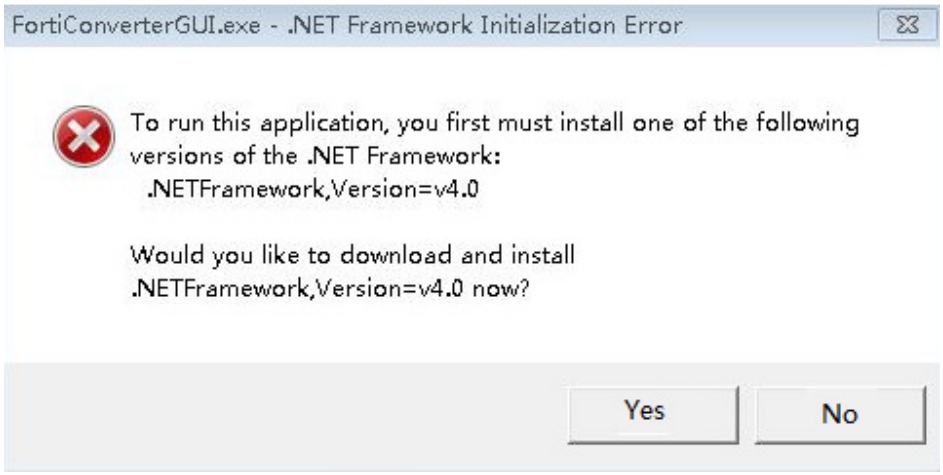


5. Select Finish to exit the FortiConverter Setup Wizard.

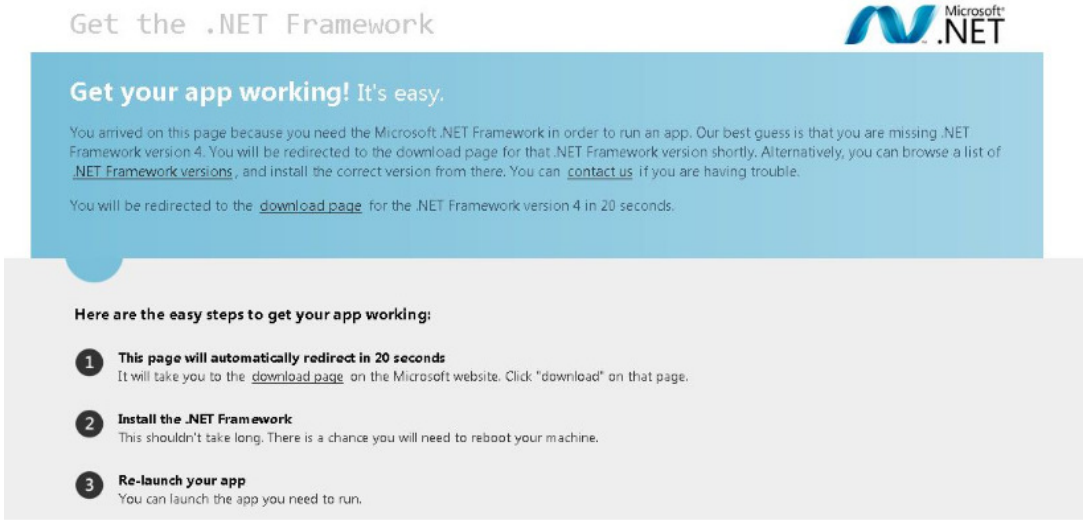
6. To launch FortiConverter, double-click the desktop shortcut icon.

System Preconditions

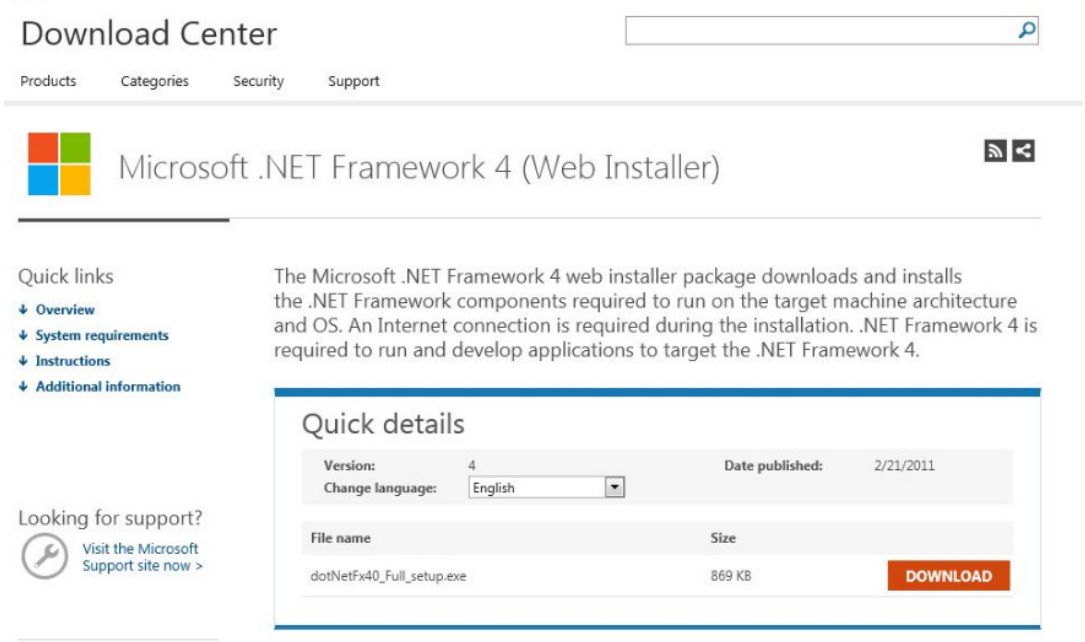
Microsoft dotnet framework4.0 is needed for the running of FortiConverter. Installation is prompted for unsupported systems. Please follow its lead.
Press *Yes*



It will link you to the Microsoft download website



Press *DOWNLOAD* to start installing dotnet framework 4.0



For better visual effect

Enable Aero in Windows 7/ Windows 8

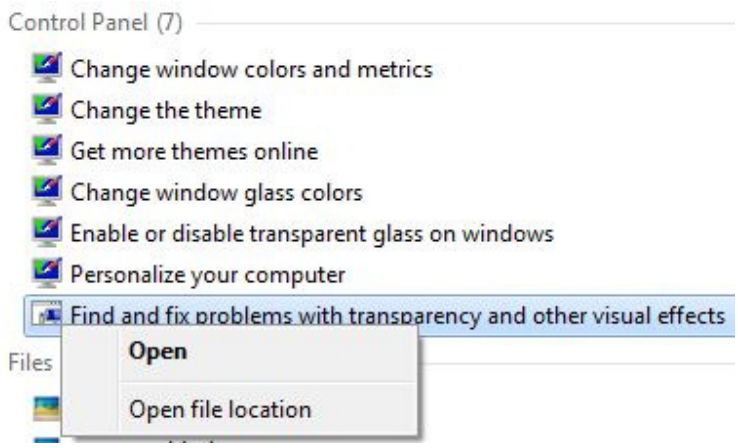
To display Aero effects such as transparency in Windows 7, follow these steps:

1. Make sure that **Windows Experience Index** has been calculated and computed.
2. Click on **Start** menu.
3. Type the following text into the Start Search box:

Aero

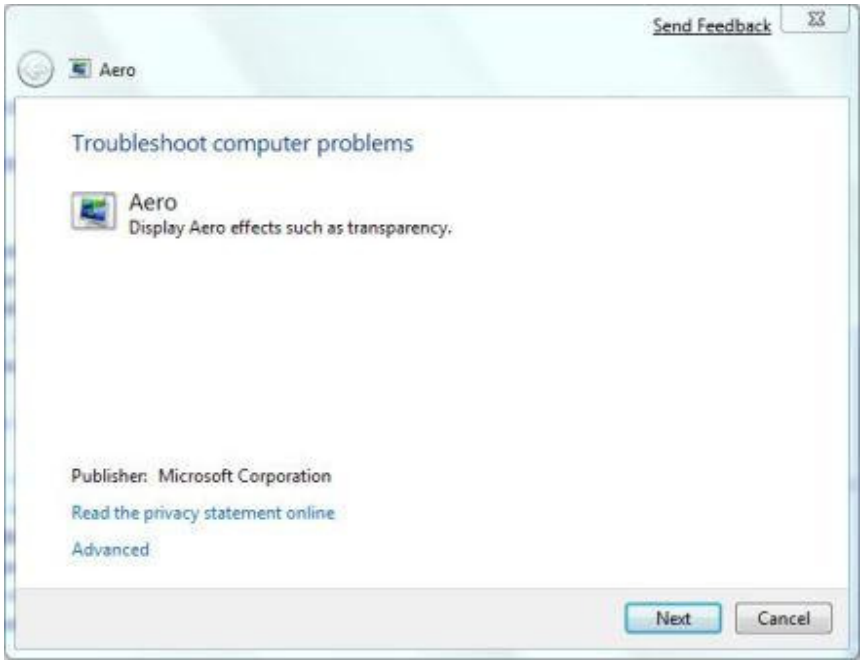
4. Click on a search result listing under Control Panel group that named as the following:

Find and fix problems with transparency and other visual effects

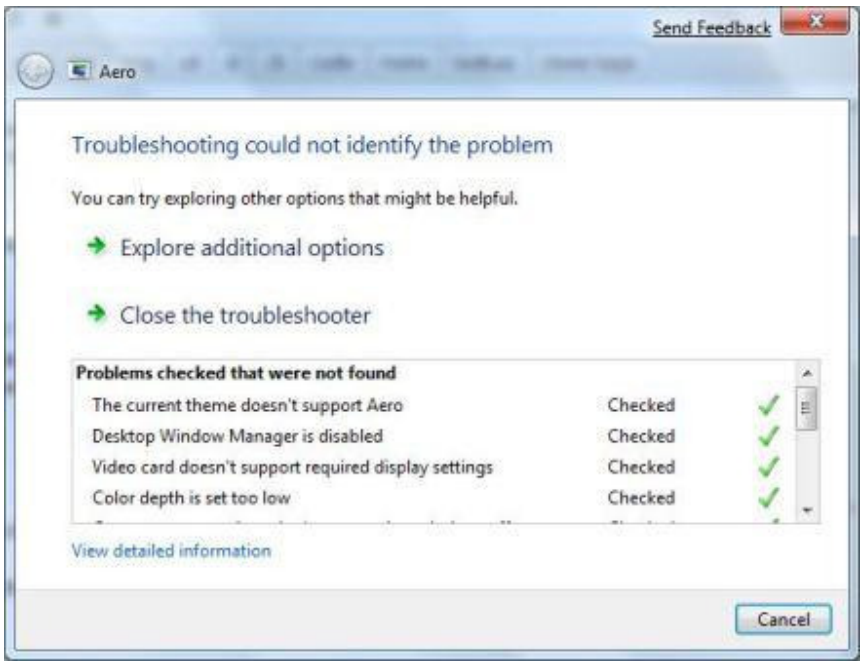


Trick: If you don't see "Find and fix problems with transparency and other visual effects" in the search results, click on **Control Panel** to see all Aero related items in Control Panel.

5. An "Aero – Troubleshoot computer problems" wizard dialog will appear. Click on **Next** button.



6. The troubleshooting wizard will try to detect any problem by running a series of checks against various components required to make Aero works and running, such as video memory, Desktop Windows Manager (DWM) service, color depth, theme, power settings and etc. At the end of the analysis, the wizard will attempt to fix the issues related to Aero service and restart the Aero feature.



Tip: If there are still items that are marked with red cross which indicates is the problems that prevent Aero from working properly, fix the issues and then rerun the “Find and fix problems with transparency and other visual effects” troubleshooting wizard again.

Resolved Issues

Bug ID	Description
0216071	Cannot convert time objects within Checkpoint firewall rule
0212680	Cisco IPSec VPN SA lifetime settings and transform-set translation error.
0216070	Generate two zones to simplify IOS EZVPN conversion
0216068	Restore “unconverted objects” web page for Checkpoint conversion
0216067	Cannot convert time objects within Checkpoint firewall rule
0215850	Cisco PIX username cannot be converted
0213930	Cannot parse netmask value from static nat command “static (inside,outside) proxy1 proxy2 dns netmask 255.255.255.255”
0216065	IOS "ip nat" command refer to "inside" or "outside" interface(s) group
0215854	Cisco EZVPN configuration's DHCP address pool cannot be converted.
0216568	Firewall Object missing for ACL Object

Pre-Conversion Technical notes

Check Point Configuration File

Check Point conversion require three files:
1. Object definition file (‘objects_5_0.c’ or 'objects.c')
2. Policy and Rule definition file (‘*.w’ or ‘rulebases_5_0.fws’)
3. Route information
4. [Optional] User and User Groups file (fwauth.NDBx)

Object definition file:
This file contains the object definition for the Check Point Firewall. The file name is objects.C(Check Point 4.x) or objects_5_0.C (Check Point NG/NGX).

Policy and Rule Definition File:
This file contains the policy or rule definition for the Check Point Firewall. The file name is <rule>.W (default Standard.W). or rulebases_5_0.fws
You can get those files in the directory of "[SmartCenter]\fw1\conf\".

Route Information:
In order to correctly interpret the network topology being converted you can provide routing information in addition to that available in the configuration file.
This information should be provided as a simple TXT file.
You can use the 'route print' command to get the information required to create the route file.
There are codes in the output that tell you if it is a directly connected interface, a host route, a network route, and so forth. The output varies depending on the platform.

Cisco Configuration File

Configuration File:
Run the "show running-config" command in the admin console of the Cisco device.
Copy the output content and paste in a TXT file.

Juniper Configuration File

Get configuration file from WebUI:
Configuration file can be obtained from the WebUI: Configuration -> Update -> ConfigFile,

Get configuration file from CLI
Run the "get conf" command in the admin console of the Cisco device.
Copy the output content and paste in a TXT file.

Sonicwall Configuration File

Configuration File (*.exp):
Configuration file can be obtained from the WebUI: **.**
System->Settings->Export Settings

Conversion Caveats

General

For some of the cases, where interfaces/addresses and service match completely, NAT will be automatically be merged into the policy.

All Polices with a number starting at 100000 are pure NAT policies which must be manually merged, and always placed at the bottom, below all security policies.

When selecting a NAT item, FortiConverter will calculate all correlated and listed policies, for the user to manually apply NAT to security policies.

This will be enhanced in a future release to enable step by step automation of this process.

Check Point

Interface "allow access" is not supported by Check Point. Default enable all services for interface.

Interface "Lead to Internet" option is equal to default gateway route.

When convert Check Point VPN configuration, the "Lead to Internet" interface will be referred as VPN policy's destination interface. If user changed the default gateway route's interface by wizard, they may need to update VPN/Policy configuration manually.

Time schedule

Support these three types "by day in month", "by day in week", "none".

The type "by day in month" will be converted to Fortinet “once” schedule.

The types "by day in week" and "none" will be converted to Fortinet “recur” schedule.

User need to assign the year range for Check Point "by day in month" time object.

If the specific day does not exist for certain month, we will not generate the “once” schedule.

For example, if user configured Check Point "by day in month" time object with below parameters.

1. For each year

2. Month: Jan./Match/Sept.

3. Day: 1, 5, 31

4. Start and end time: 0:00 to 10:00

If user had assigned year range value 1 by wizard, and had got current year value 2013 from local PC which run the wizard.

The output content for Fortinet will be this:

Once Schedule list:

From 0:00 Jan/1/2013 To 10:00 Jan/1/2013

From 0:00 Jan/5/2013 To 10:00 Jan/5/2013

From 0:00 Jan/31/2013 To 10:00 Jan/31/2013

From 0:00 Match/1/2013 To 10:00 Match/1/2013

From 0:00 Match/5/2013 To 10:00 Match/5/2013

From 0:00 Match/31/2013 To 10:00 Match/31/2013

From 0:00 Sept./1/2013 To 10:00 Sept./1/2013

From 0:00 Sept./5/2013 To 10:00 Sept./5/2013

<---------- notice that Sept. 31 does not exist ---------->

Check Point support firewall rule action with "Client Auth" option, this option will be converted to Fortinet “user-identity” policy with “accept” action.

Static NAT object for Check Point is 1-to-1 IP mapping relationship; this transform action should be applied to bi-direction traffic. After converting to Fortinet source NAT policy, the policy with IP pool is not restrict to 1-to-1 IP mapping relationship.

Check Point VPN is not configured within firewall rule. After convert to Fortinet configuration, we will generate several VPN policies from "Intranet" interfaces to "Lead to Internet" interface.

Juniper

Interface name leading by "vlan" will be recognized as logical interface.

For a Juniper-ScreenOS configuration which already has NAT that is configured inside a policy, it will be automatically converted. NAT fine-tuning is not required.

Cisco

Cisco “object-group” contains two types of services. Because Fortinet service contains both source and destination port definition for traffic, only type "service-object" can be converted to Fortinet service directly. The other type "port-object" cannot be converted directly. We will generate Fortinet service object from ACL's protocol and source / destination services configuration.

Cisco IPSec VPN phase 1 ISAKMP can support these three methods, "pre-share", "rsa-sig" and "dsa-sig". Fortinet only support the first two methods. Cisco "dsa-sig" will be translated to "rsa-sig".

If Cisco ISAKMP defined more than one method within the configuration the user needs to assign the method for each VPN connection by use of the wizard. Cisco EZVPN configuration will be converted to Fortinet VPN policies with from “Intranet” interfaces, to interface which assigned by VPN crypto map interface command.

Sonicwall

Because Fortinet does not support special characters like ‘#’, ‘(’ and ‘)’, we use these characters ‘*’, ‘[’ and ‘]’ to replace them correspondingly.

For example, address book with name “SNWL #1” will be translated to “SNWL *1”; and service book with name "Citrix TCP (Session Reliability)” will be translated to "Citrix TCP [Session Reliability]".

Fortinet does not support MAC configuration for address book, so the related address book objects cannot be converted.

Default address book “Any” represent all IP address for SonicWall firewall. We will generate an address book “Any” for Fortinet.

Fortinet address/service group object should be configured with at least one member. If SonicWall configuration contains an empty address/service group object, address “_Address_Null” or service “_Service_Null” will be generated and referred by the empty address/service group.

There is small difference between SonicWall and Fortinet schedule group. SonicWall schedule group can include only one “onetime” schedule and multiple “recur” schedules. The “onetime” schedule is an implicit object which can be embedded into the schedule group. But Fortinet cannot support this implicit attribution, every object (onetime or recur) which can be referred by schedule group need to be defined explicitly. This difference leads to some auto-generated “onetime” schedules within the configuration output.

Fortinet “onetime” or “recur” time schedule cannot support a time value “24:00” (equal to the next day’s 00:00). When converting SonicWall time schedule “M 00:00 to 24:00”, we need to set the end time with “00:00”.

Local user’s password is a cipher string therefore we just set local user’s password as “123456”.

Nested user group is not supported.

For example, there are two user groups with the name “group1” and “group2”, and “group1” belongs to “group2”. SonicWall user group can support this nested configuration; Fortinet’s user group does not support this feature. After converting user group “group2”, there will be an empty user group “group2”.

Cannot convert tunnel routes (static route with the next hop tunnel interface).

Cannot convert IPSec VPN/tunnel conversion.

NAT rule conversion constraint.

Because Fortinet configure NAT rules within a policy module, each SonicWall NAT rule will be converted to one policy entry. If the NAT rule's status is enabled, then the converted policy status also set to enabled. The converted policy ID for NAT rule starts from 100001. The regular firewall policy ID starts from 10000.

For source NAT rule, we will create a new IP pool object for Fortinet policy's source address.

For example, SonicWall source NAT rule looks like below.

Org Src	Tran Src	Org Dest	Tran Dest	Org Serv	Tran Serv
All Interface IP	X2 IP	Any	Original	Any	Original

After converting to the Fortinet configuration, a new IP pool object with name "ippool-X2 IP" will be created, we simply add a prefix "ippool-" before the translated source address book "X2 IP".

For destination NAT rule, we will create a new VIP object for Fortinet policy's destination address.

For example, Sonicwall's destination NAT rule like below.

Org Src	Tran Src	Org Dest	Tran Dest	Org Serv	Tran Serv
LAN Subnets	Original	WoW Static IP	X0 IP	SSLVPN	Original

After converting to Fortinet configuration, a new VIP object with name "vip-X0 IP" will be created, we just add a prefix "vip-" before the translated destination address book "X0 IP".

There is a constraint for destination NAT configuration, Fortinet destination NAT only supports VIP and VIP group. The VIP object is restricted to 1-to-1 address and port mapping between the external and internal network. But SonicWall does not have this constraint for destination NAT rule.

For example, SonicWall source and destination NAT policy like below.

Org Src	Tran Src	Org Dest	Tran Dest	Org Serv	Tran Serv
test_1112_grp	test_11_gw	test_12_gw	test_1211_grp	Echo	Original

Address book "test_12_gw" only contains one IP address, but address group "test_1211_grp" contain two address members "test_11_gw" and "test_12_gw".

This nat rule will translate IP packet's destination address from address book "test_12_gw" to address group "test_1211_grp". Fortinet cannot generate VIP object for this nat rule, because

the address book “test_12_gw” and the address group “test_1211_grp” contains different counts of IP addresses.

Known Issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please contact fconvert_feedback@fortinet.com.

Known Bug References

Table 1: Known issues.

Bug ID	Description
N/A	No Support for Cisco ASA twice NAT. Implemented in Cisco ASA 8.3